Elektronische Signatur

Zwei Schlüssel bringen Sicherheit

Zu Beginn des Jahres ist ein neues und weithin beachtetes Gesetz in Kraft getreten, das „Bundesgesetz über die elektronische Signatur, ZertEs". Nun ist es beileibe keine bahnbrechende Neuerung, die digitale Kommunikation mittels elektronischer Signatur zu sichern – was genau ändert sich also durch das neue Gesetz?

Um es gleich vorweg zu nehmen: Einschneidende Änderungen im praktischen Gebrauch ergeben sich in der Tat nicht, doch soll die Gelegenheit nicht ungenutzt bleiben, die möglichen Anwendungsgebiete und das dahinter verborgene Potential gerade auch für KMU einmal etwas genauer unter die Lupe zu nehmen. Und natürlich zu erläutern, was sich nun wirklich verändert hat. Zuerst ist zu klären, wofür die Zertifikate, die für die elektronische Signatur benötigt werden, verwendet werden können. Sie dienen zum Beispiel dazu, die Authentizität und Integrität einer Nachricht bzw. eines Dokuments sicherzustellen. Sprich: Die elektronische Signatur erlaubt es, ein Dokument eindeutig einem Absender zuzuordnen und zu gewährleisten, dass es auf dem Weg von A nach B nicht verändert wurde. Noch nicht garantiert ist dabei die Vertraulichkeit: Wer

ein Dokument versenden möchte, ohne dass es von einem Dritten unerwünscht eingesehen werden kann, muss es verschlüsseln. (Wie genau diese beiden Vorgänge ablaufen, erfahren Sie im Kasten „Funktionsweise der elektronischen Signatur“.) Anwendung findet dies längst zum Beispiel im E-Banking oder bei der Bestellung von Produkten über Online-Shops.

Signieren in der Schweiz, akkreditieren im Ausland?

Um den Luxus der sicheren Kommunikation aber selbst geniessen zu können, benötigt man ein Zertifikat, das von verschiedenen Anbietern wie etwa Thawte oder VeriSign, um zwei populäre Beispiele zu nennen, erhältlich ist. Für Privatanwender bedeutet dies einen nicht zu unterschätzenden Aufwand: Sie müssen zuerst via Internet persönliche Daten angeben, darunter nicht zuletzt die Nummer des Reisepasses. Da sämtliche Anbieter ihren Sitz im Ausland haben, sind die Daten bei z.B. von Thawte autorisierten Stellen in der Schweiz zu verifizieren, was durchaus zu einer kleinen Odyssee führen kann. Unternehmen haben es etwas einfacher: Sie beantragen das Zertifikat ebenso unter Angabe der wichtigsten Informationen per Internet. Zur Bestätigung genügt jedoch eine Kopie des Handelsregisterauszugs, die per Fax an den jeweiligen Anbieter verschickt wird.

In beiden Fällen gilt allerdings: Die Zertifizierungsstelle sitzt im Ausland, nicht in der Schweiz. Genau an diesem Punkt kommt auch das neue Bundesgesetz ins Spiel – es bereitet nämlich den Boden für eine Schweizer Zertifizierungsstelle. Eine solche gab es mit der von mehreren Banken getragenen Firma Swisskey zwar schon einmal, doch das Projekt wurde damals aus finanziellen Gründen wieder eingestellt.

Mehr über die Vorteile einer eigenen Zertifizierungsstelle und die potentiellen Anwendungen der elektronischen Signatur im KMU-Bereich erfahren Sie im Interview mit Andreas Wisler, Fachmann für IT-Security.

Im Interview

Andreas Wisler (Tel. 052 320 91 20) ist Geschäftsführer der GO OUT Production GmbH, einem IT-Sicherheitsdienstleister mit Sitz in Wiesendangen. Er unterrichtet in der Klubschule Migros den Lehrgang „IT-Security Manager“, darüber hinaus veröffentlicht er regelmässig die Infonews zu aktuellen Sicherheitsthemen. Dieser informative Newsletter kann kostenlos und unverbindlich auf www.goSecurity.ch bestellt werden.

„Ein Zertifikat einzubinden ist eine Aufgabe von wenigen Minuten.“

Wer – oder welche Organisation – kommt Ihrer Meinung nach als Schweizer Zertifizierungsstelle in Frage?

A. Wisler: Da gibt es zwei Varianten. Zum einen gibt es Anbieter im Ausland, die seit Jahren Zertifikate ausstellen und nun natürlich auch versuchen, die Anerkennung für die Schweiz zu bekommen. Zum anderen bleibt zu hoffen, dass aus dem Schweizer Markt eine Firma entsteht, die diese Aufgabe übernimmt. Im Moment sieht es nicht so aus, als würde in dieser Hinsicht sofort etwas passieren. Bis zum Sommer werden wir sicher warten müssen. Allerdings ist schon eine so genannte SAS, eine Schweizer Akkreditierungsstelle, eingerichtet. Dabei handelt es sich konkret um KPMG Fides Peat, die somit zwar nicht selbst Zertifikate ausstellen, aber entsprechend dem neuen Bundesgesetz Zertifizierungsstellen akkreditieren kann. Wenn sich nun also ein Unternehmen findet, das als Zertifizierungsstelle fungieren will, so wird KPMG Fides Peat überprüfen, ob alle gesetzlichen Voraussetzungen erfüllt werden.

Verträge per Postkarte verschicken?

Wo sehen Sie vor allem für KMU die wichtigsten Einsatzmöglichkeiten der elektronischen Signatur?

A. Wisler: Das Hauptanwendungsgebiet ist meines Erachtens die sichere Kommunikation. E-Mails sind ja beinahe wie Postkarten, die übers Internet verschickt werden – sie sind theoretisch für jeden einsehbar. Wenn ich mein Mail verschlüssele, habe ich die Garantie, dass es tatsächlich nur vom Empfänger gelesen werden kann. Angehängte Dokumente werden damit ebenfalls sozusagen unsichtbar. Bei der reinen Signatur ist das anders: Dokumente werden nicht verschlüsselt, doch es besteht die Garantie, dass sie tatsächlich von einer bestimmten Person erstellt und signiert wurden und keine Veränderungen stattgefunden haben. Dies ist zum Beispiel bei Verträgen interessant, die online versendet werden.

Hier ist der grosse Vorteil, dass die Mechanismen etwa in der Microsoft-Umwelt bereits bestehen. Nehmen wir einmal Outlook: Ein Zertifikat einzubinden ist eine Aufgabe von wenigen Minuten; ab diesem Moment werden alle Mails signiert bzw. verschlüsselt verschickt, je nachdem, welche Variante man wählt. Das Gleiche gilt für Word- oder PDF-Dokumente.

So überzeugend und sicher das klingt: Was geschieht, wenn mein privater Schlüssel entwendet wird? Oder der eines Geschäftspartners – so dass ich vielleicht gar nicht weiss, dass die Kommunikation nicht mehr sicher ist …

A. Wisler: Es kann natürlich passieren, dass ein Zertifikat kompromittiert wird, sei dies durch Diebstahl, Zerstörung oder einen anderen Zugriff von aussen. Für diesen Fall gibt es die Möglichkeit, das Zertifikat bei der Zertifizierungsstelle sperren zu lassen. Zu diesem Zweck werden so genannte CRLs (Certificate Revoke Lists) geführt, die über alle gesperrten Zertifikate Auskunft erteilen und von den Websites der jeweiligen Anbieter gratis herunter geladen werden können. Es ist meiner Meinung nach ein Problem, das noch zu wenige Programme diese Listen automatisch holen. Nehmen wir einmal Windows als Beispiel: Windows Server 2003 aktualisiert selbständig, XP dagegen tut dies nicht.

„Es hat sich herauskristallisiert, dass das System nicht funktioniert, wenn der User zu viel damit zu tun hat."

Grosses Potential bleibt ungenutzt

Haben Sie einen Überblick, ob die elektronische Signatur von KMU in der Schweiz überhaupt genützt wird?

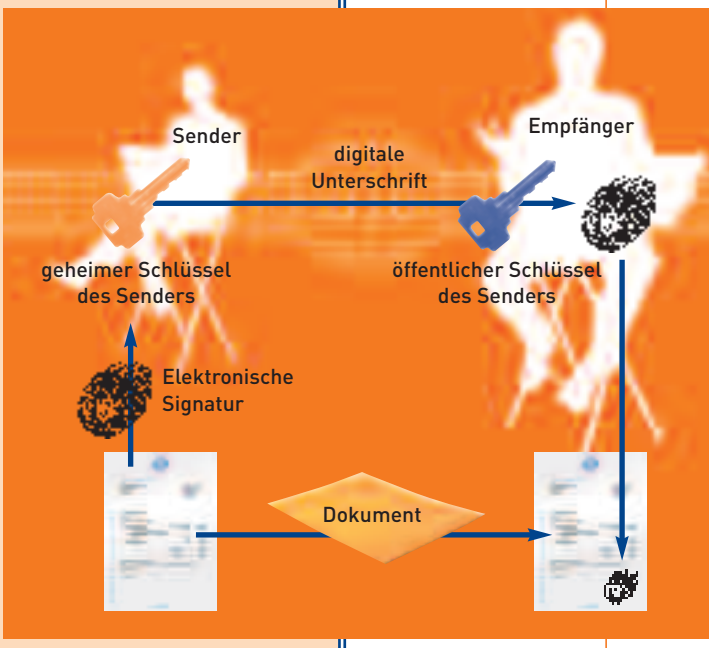
A. Wisler: Für die Kommunikation via Internet kann man das mit ja beantworten. Sei es nun, dass Firmen untereinander über VPN miteinander verbunden sind, oder Shops bzw. Bankverbindungen durch ein SSL-Zertifikat geschützt werden – diese Möglichkeiten werden von vielen Firmen aktiv genutzt.

Anders sieht es aus, was die reine Signatur bzw. das Verschlüsseln von Dokumenten angeht. Ich würde behaupten, dass KMU dies bisher mehr oder weniger gar nicht nutzen. Das liegt vermutlich auch an den Fragen, die man sich dabei stellen muss, wie etwa: Was passiert mit dem Zertifikat eines Mitarbeiters, wenn er aus der Firma ausscheidet? Können seine verschlüsselten Dokumente überhaupt noch verwendet werden?
Viele Anbieter in unserem Bereich versuchen aber, die elektronische Signatur zu pushen, indem sie fertige Lösungen anbieten, die in den Mail-Server integriert werden können. Es hat sich herauskristallisiert, dass das System nicht funktioniert, wenn der User zu viel damit zu tun hat, deswegen soll ihm so die Arbeit abgenommen werden. Ich persönlich bin überzeugt, dass hier ein grosses Potential liegt und gerade solchen fertigen Server-Lösungen die Zukunft gehört.

Vielen Dank für das Interview

Funktionsweise der elektronischen Signatur

Das elektronische Signieren eines Dokuments dient dazu, den Absender eines Dokuments eindeutig zu identifizieren und die Integrität des Dokuments zu überprüfen. Hierzu benötigt der Absender zwei Schlüssel, den public key und den private key. Der private Schlüssel darf niemandem zugänglich gemacht werden. Er dient dazu, aus dem Dokument einen Hash-Wert zu generieren, also einen Wert, der eindeutig nur aus diesem Dokument und mit diesem Schlüssel entsteht. Gleichzeitig stellt der Absender dem Empfänger seinen öffentlichen Schlüssel zur Verfügung, anhand dessen dieser über besagten Hash-Wert überprüfen kann, ob das Dokument tatsächlich authentisch ist. Käme es von einem anderen Absender oder wäre es verändert worden, so wäre dies am veränderten Hash-Wert zu erkennen.



Blickpunkt:KMU
Infografik

Für das Verschlüsseln einer Nachricht ist das Vorgehen genau umgekehrt: Der Absender benötigt den öffentlichen Schlüssel des Empfängers, um ein Dokument zu verschlüsseln. Dieses kann nur noch mit dem privaten Schlüssel des Empfängers entschlüsselt werden, selbst der verwendete öffentliche Schlüssel lässt es nicht zu, das Verfahren rückgängig zu machen. Somit ist sichergestellt, dass definitiv nur der gewünschte Empfänger das Dokument wieder in Klartext verwandeln kann. Für den Umgang mit den eigenen Schlüsseln bedeutet dies: Der private key ist unter allen Umständen vor Fremdzugriff zu schützen. Gerät er in falsche Hände, so können Dritte Dokumente im Namen des eigentlichen Besitzers signieren und/oder für ihn bestimmte, verschlüsselte Dokumente einsehen. Der public key hingegen kann vom Benutzer sogar auf der eigenen Website publiziert werden, da er Empfängern von signierten Nachrichten dazu dient, diese auf Authentizität und Integrität zu prüfen sowie anderen die Möglichkeit gibt, Dokumente so verschlüsselt an den Benutzer zu senden, dass nur er sie einsehen kann.